AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION

# ORGANISED CRIME IN AUSTRALIA 2017

# ORGANISED CRIME IN AUSTRALIA 2017

# FOREWORD

## THE GLOBAL BUSINESS OF ORGANISED CRIME

The Australian Criminal Intelligence Commission (ACIC) commenced operations on 1 July 2016 bringing together the Australian Crime Commission and CrimTrac as one agency, along with the research capability of the Australian Institute of Criminology (AIC).

This publication is the first *Organised Crime in Australia* (OCA) report produced by the newly formed ACIC and provides an update to information published in the Australian Crime Commission's *Organised Crime in Australia 2015* report.

The *Organised Crime in Australia 2017* (OCA 2017) report provides a snapshot of serious and organised crime in Australia, exploring existing and emerging organised crime threats affecting the Australian community and national interests. Information presented in the OCA 2017 is intended to inform readers of the current trends in Australian crime markets and to provide information on how the Australian Government is addressing the threat of serious and organised crime to Australia.

Serious and organised crime touches the lives of Australians in unprecedented ways. It is destructive, pervasive and complex. In December 2015, the then Australian Crime Commission estimated the cost of serious and organised crime in Australia to be at least A$36 billion a year. That equates to A$1,561 out of every individual Australian's pocket and adds 6.3 per cent to the average cost of living.

Alongside the financial cost of serious and organised crime are the devastating health and social impacts of illicit drug use. There are also the highly visible flow-on effects of serious and organised crime activity on the Australian community, typically in the form of volume crime.

Serious and organised criminals control illicit markets that terrorists may seek to access to enable acts of terrorism. Links have been observed between serious and organised crime and persons of interest to counter-terrorism investigations.

Organised crime in Australia is proficient and enduring. It is transnational in nature, technology enabled and increasingly functions as a business: employing professionals; outsourcing key activities such as money laundering; diversifying into multiple criminal markets; and developing strong, consistent revenue streams through involvement in comparatively low-risk activities.

Geographic boundaries no longer contain criminal networks. Increasing access to and uptake of the internet provides serious and organised crime groups with the ability to target thousands of Australians simultaneously from anywhere in the world. Transnational organised crime groups continue to be attracted to and target Australia's lucrative illicit drug market.

As the reach of organised criminals expands to exploit markets offshore, law enforcement has also become more connected through the development of information-sharing platforms and enhanced relationships with overseas partner agencies, to effect timely information sharing on key threats and engage in joint disruptive activity.

Collaboration is occurring on national and international levels between industry, governments and law enforcement to ensure informed, considered and innovative responses to the threat of organised crime. With ACIC intelligence indicating up to 70 per cent of Australia's serious and organised crime threats are based offshore or have strong offshore links, and as visibility of criminal activities becomes increasingly obscured through new technologies and sophisticated methods, it is clear that a connected, informed and collaborative response to the threat is required.

Nicole Rose PSM
Acting Chief Executive Officer
Australian Criminal Intelligence Commission

# SNAPSHOT

## GLOBAL BUSINESS OF ORGANISED CRIME

**Transnational**

- exploits lucrative markets from locations offshore

**Technology enabled**

- provides access to victims all over the world

**Operates as a business**

- employs the services of **professionals** to advise on complex methods and techniques
- outsources key activities such as money laundering to dedicated **service providers** and **professional organisations**
- **diversifies** into multiple criminal markets to permit responsiveness to shifts in supply and demand
- ensures a strong, **consistent revenue stream** through involvement in comparatively low risk markets to finance the higher risk, more lucrative aspect of their business
- **proficient and enduring**

## HIGHLIGHTS

**Key enablers**

- technology and digital infrastructure
  - **encrypted** communication
  - highly networked and connected criminals
- professional **facilitators**
- **money laundering organisations**
  - professional money laundering organisations and offshore service providers

**Market shifts**

- predicted rise in **cocaine** supply
- use of **opioids** and **fentanyl** at concerning levels

**Key threats**

- **methylamphetamine** is an illicit drug of disproportionate harm in Australia
- exploitation of **financial sector** poses a significant risk to the integrity of the Australian economy
  - **cyber enabled**

- manipulation of Australia's **visa and migration** system presents an ongoing threat to Australia's borders
- **growing internet** availability and usage increases organised crime access to **vulnerable individuals**

## RESPONSES

**Informed**

- *Organised Crime in Australia* report
- *National Organised Crime Response Plan 2015–18*
- *National Wastewater Drug Monitoring Program*
- *The National Ice Taskforce and National Ice Action Strategy 2015*

**Collaborative**

- Task forces and joint agency groups
- Five Eyes Law Enforcement Group

**Connected**

- National Criminal Intelligence System
- National Policing Systems

# CONTENTS

CEO FOREWORD ..... 1
Executive Summary ..... 5
How we are Responding ..... 6
KEY ENABLERS ..... 8
Theme Summary ..... 8
Money Laundering ..... 8
Technology ..... 11
Professional Facilitators ..... 12
Identity Crime ..... 13
Public Sector Corruption ..... 14
Violence and Intimidation ..... 15
ILLICIT COMMODITIES ..... 16
Drug Market Summary ..... 16
Methylamphetamine ..... 16
Precursor Chemicals ..... 17
Cocaine ..... 18
MDMA ..... 19
Cannabis ..... 20
Heroin ..... 20
Illicit Pharmaceuticals ..... 20
Tryptamines ..... 21
New Psychoactive Substances ..... 22
Anaesthetics ..... 22
Performance and Image Enhancing Drugs ..... 23
Illicit Tobacco ..... 23
Illicit Firearms ..... 24
SERIOUS FINANCIAL CRIME ..... 27
Theme Summary ..... 27
Cybercrime ..... 27
Investment and Financial Market Fraud ..... 30
Revenue and Taxation Fraud ..... 32
Superannuation Fraud ..... 33
Card Fraud ..... 35
SPECIFIC CRIME MARKETS ..... 36
Theme Summary ..... 36
Visa and Migration Fraud ..... 36
Environmental Crime ..... 38
Intellectual Property Crime ..... 40
CRIMES AGAINST THE PERSON ..... 41
Theme Summary ..... 41
Sexual Exploitation of Children ..... 41
Human Trafficking and Slavery ..... 43

# EXECUTIVE SUMMARY

**Transnational serious organised criminal groups** have had a significant impact on crime markets in Australia in the past two years, with **technology and digital infrastructure** presenting as key enablers across multiple crime types. Australia's borders face ongoing challenges from transnational organised crime and the movement of illicit goods, money and people. However, for some crime types, technology has dissolved borders that previously protected victims from offshore offenders.

The use of technology and digital infrastructure by serious and organised crime is considered a key determinant of significant changes in the criminal landscape into the future. The impact of the availability of technology can already be seen in multiple crime types, with greater instances of **technology-enabled fraud** in the areas of online banking, trade, superannuation and identity crime. The ability to target individuals remotely from any location in the world is attractive to serious and organised crime groups, who actively use technology to target the financial sector, to undertake online trading of illicit goods via the **darknet,** and to commit acts of **child sexual exploitation** (CSE) through online grooming and distribution of child exploitation material (CEM). The growing availability and usage of the internet has also increased access by organised crime to vulnerable individuals.

The ready availability of technology to reduce law enforcement visibility of serious and organised crime groups' activities has had an impact on how law enforcement agencies undertake their work. The rapid uptake of new capabilities such as **encrypted communication** devices and applications will continue to challenge law enforcement in coming years.

**Professional facilitators** have emerged as a fundamental issue for law enforcement and regulatory agencies. In an increasingly complex global environment, criminals engage a range of professional facilitators to commit crimes, avoid detection and conceal assets.

**Money laundering** continues to be a significant enabler of criminal activity, with recent joint targeting of professional money laundering organisations by domestic and international partner agencies revealing the significance and international dimension of this threat.

Over the past few years, the speed with which global trends have been replicated in Australia has increased. International law enforcement partners predict that a significant increase in coca cultivation in Colombia will result in cocaine supply to the United States increasing to levels not seen in the past 10 years. Significant detections of **cocaine** in Australia in late 2016 and early 2017 may suggest an expansion of this market in Australia. Agencies in the United States and Canada report concerns with opioid abuse and a rise in the use of fentanyl. Results of the ACIC's National Wastewater Drug Monitoring Program (NWDMP) in 2017 indicate oxycodone and **fentanyl** consumption (licit and illicit) across all jurisdictions is at concerning levels.

**Methylamphetamine**[1] use is of ongoing concern and is considered by the ACIC as an illicit drug of disproportionate harm in Australia. The results of the NWDMP identify methylamphetamine as the highest-consumed illicit drug tested across all regions in Australia, with Australia ranking second for the consumption of methylamphetamine when compared with 17 European countries with comparable reported data.

1 The word 'methylamphetamine' is used in this report to describe the various forms of methylamphetamine including crystal methylamphetamine (commonly referred to as 'ice') and methamphetamine, unless specifically referenced.

The expansion of serious and organised crime activity in the **financial sector** poses a significant risk to the integrity of the Australian economy, financial markets, regulatory frameworks and revenue collection. Finally, manipulation of Australia's **visa and migration system** presents ongoing challenges to the security of the border, as transnational organised crime seeks to enable the movement of people, money and illicit goods in support of criminal enterprise.

# HOW WE ARE RESPONDING

The *National Organised Crime Response Plan 2015–2018* articulates Australia's national response to the threat posed by serious and organised crime. Current responses to serious and organised crime recognise the growing international dimension of the threat and the need for strong partnerships with domestic and international agencies. Initiatives require a coordinated national and international approach that harnesses collective resources, capabilities, expertise and knowledge.

The following provides a summary of some of the key initiatives from the *National Organised Crime Response Plan 2015–2018* and other recent strategies aimed at reducing the threat from serious and organised crime and its impact on the Australian community.

## INFORMED

- National Wastewater Drug Monitoring Program—funding allocated in 2016 to implement the NWDMP. The program will analyse wastewater over a three-year period to provide a measure of the demand for a range of licit and illicit drugs. Results of the NWDMP will inform governments and effectively direct resources to priority areas.
- National Ice Taskforce—established by the Australian Government in April 2015. Taskforce findings informed the development of the *National Ice Action Strategy 2015*, endorsed by the Council of Australian Governments in December 2015. The strategy aims to reduce the prevalence of ice use and resulting harms in the Australian community.

## COLLABORATIVE

**Task force and joint agency arrangements**

- initiatives of the Serious and Organised Crime Coordination Committee including ACIC Task Force Morpheus[2] focusing on activities of outlaw motorcycle gangs (OMCGs) and Operation Athena targeting the illegal firearms market
- intelligence hubs including the Australian Gangs Intelligence Coordination Centre (AGICC)[3] and the National Criminal Intelligence Fusion Capability
- Task Force Vestigo[4] created to enhance international engagement and collaboration in responding to the threat posed to Australia by high-risk serious and organised crime entities either based overseas or with direct links to criminal entities based overseas
- international collaboration through involvement in the Five Eyes Law Enforcement Group (FELEG)
- Serious Financial Crime Taskforce (SFCT), specifically targeting fraud, money laundering and defrauding the Commonwealth

2 Morpheus is a joint law enforcement initiative across Commonwealth and national law enforcement, with a focus on outlaw motorcycle gangs (OMCGs) that pose a high risk to the Australian community.
3 The AGICC provides a dedicated intelligence capability for the AFP-led National Anti-Gangs Squad (NAGS).
4 Established November 2016.

- Australian Transaction Reports and Analysis Centre (AUSTRAC) memorandums of understanding with the China Anti-Money Laundering Monitoring and Analysis Centre and the Jordanian Anti Money Laundering and Counter Terrorist Financing Unit to facilitate the exchange of financial intelligence
- joint government and industry initiatives:
  - Fintel Alliance[5]
  - Australian Financial Crimes Exchange (AFCX)[6]
- initiatives to reduce the threat of cybercrime including:
  - *National Cyber Security Strategy*
  - Australian Cyber Security Centre
  - Participation in the International Global Operations Targeting Unit
- Increased funding for Australian Border Force Tobacco Strike Team to combat criminal syndicates attempting to smuggle illicit tobacco into Australia
- Operation Sovereign Borders, a border security operation aimed at combating maritime people smuggling and protecting Australia's borders
- Joint Anti Child Exploitation Teams working to identify online sexual predators
  - Carly's Law[7] was recently passed by federal parliament to enhance the capability of law enforcement to respond to criminals who misrepresent their age with the intent to cause harm, engage in or procure sexual activity with a minor.

## CONNECTED

Advances in technology are contributing to law enforcement's ability to discover, understand and respond to serious organised crime. Initiatives include:

- Australia's biometric Face Verification Service[8]
- ACIC's National Criminal Intelligence System (NCIS) pilot program
- technological developments—including DNA analysis, spatial monitoring software, thermal imagery, and GPS-enabled cameras and smartphones—being used in new ways to detect criminal activities
- improved monitoring of the scope of the Australian illicit firearm market including:
  - Australian Firearm Information Network[9]
  - National Firearm Identification Database[10].

5 A world-first public–private partnership established by Australian Transaction Reports and Analysis Centre (AUSTRAC) and launched in March 2017.
6 The Australian Financial Crimes Exchange (AFCX) brings together business, government, law enforcement agencies and industry groups to combat the threat from financial and cybercrime by providing leading security capabilities, technology and intelligence in one central platform
7 *Criminal Code Amendment (Protecting Minors Online) Act 2017*.
8 In November 2016, the first phase of Australia's biometric Face Verification Service became operational, providing the Department of Foreign Affairs and Trade and the Australian Federal Police access to citizenship images held by the Department of Immigration and Border Protection.
9 An ACIC-hosted viewing platform for jurisdictional firearm data, both historical and contemporary, on licit and illicit firearms located by law enforcement.
10 Online tool used by jurisdictions to standardise terminology according to industry specifications of firearms and their variants.

# KEY ENABLERS

## THEME SUMMARY

The ACIC has identified six key enablers for serious and organised crime:

- Money laundering
- Technology
- Professional facilitators
- Identity crime
- Public sector corruption
- Violence and intimidation

Key enablers have a unique role in facilitating serious and organised crime. Activities such as money laundering and identity crime contribute to the effectiveness of other types of organised crime. While not all of the above enablers are present in every illicit market, two or more enablers may be used concurrently within the same criminal enterprise.

Enablers are integral to the business of serious and organised crime groups. Law enforcement, regulatory, legislative or policy actions against enabling activities have the potential to disrupt criminal networks across multiple illicit markets or to severely hinder their activities. For example, increased law enforcement and regulatory capability to identify and prosecute professional facilitators would have a significant impact on all criminal groups relying on the expert advice and knowledge provided by such facilitators to perpetrate or conceal criminal activity. Similarly, reduced ability of crime groups to realise their illicit proceeds or conceal their illicit wealth through targeting of money laundering would be likely to affect future illicit activity by serious and organised crime groups.

## MONEY LAUNDERING

Money laundering remains a fundamental enabler of profit-motivated crime, and is a significant, potentially lucrative criminal enterprise in itself. The primary goals of money laundering are to give illicit money the appearance of legitimacy and, through the use of complex methods, to move illicit funds without detection. Illicit funds, laundered for the appearance of legitimacy, are likely to be invested in businesses or schemes that provide the greatest chance of concealing the origins of the money, rather than on the basis of predicted returns.

Money laundering is an extremely diverse activity carried out at all levels of sophistication, and it plays an important role in serious and organised crime. The banking system and money transfer services are common methods used to launder funds, and money launderers continually exploit vulnerabilities in the financial system to circumvent the counter-measures designed to detect them. Bulk cash smuggling also remains a viable and active means to launder the proceeds of crime.

The ACIC's Eligo National Task Force[11] (Eligo) identified the following four key features of money laundering activity in Australia, which can appear separately or jointly:

- intermingling legitimate and illegitimate financial activities through cash-intensive businesses or front companies
- engaging professional expertise/facilitators
- engaging specialist money laundering organisations to provide specific money laundering services to domestic and international crime groups
- 'internationalisation' of the Australian crime environment—international money laundering components for Australian crime groups are common.

## CASE STUDY: DISRUPTION OF INTERNATIONAL MONEY LAUNDERING SYNDICATE

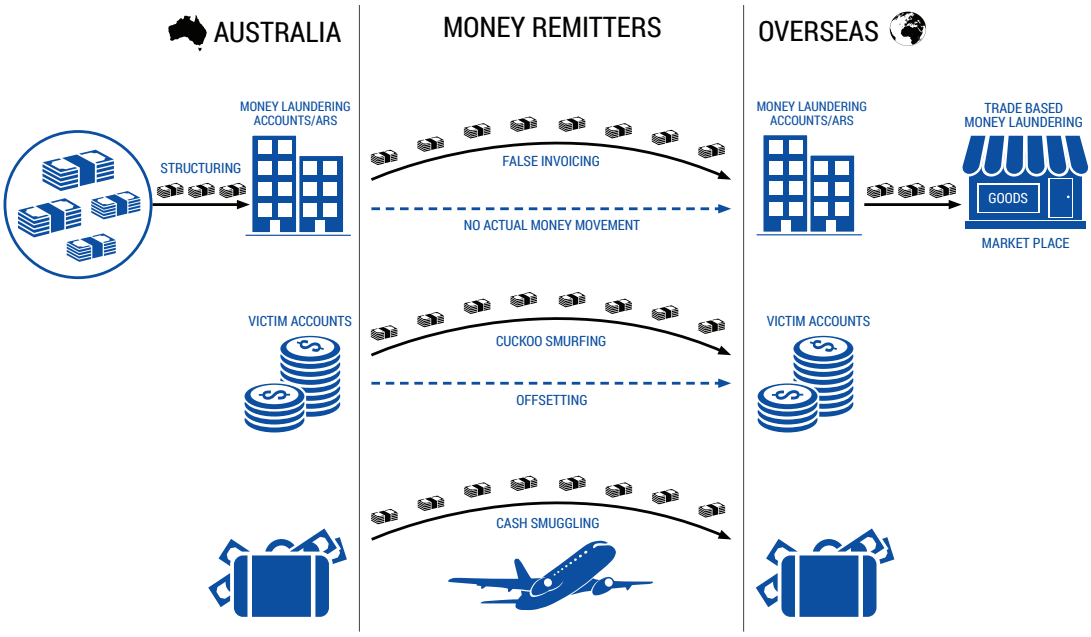
In January 2017, following a lengthy joint investigation, the key figure in an international money laundering syndicate was arrested in Sydney. The foreign national was charged with knowingly directing the activities of a criminal group. Police allege the woman coordinated the group's activities from Vietnam, recruited people to launder money, and directed them on how to acquire, deposit and exchange the funds through financial institutions.

Joint task force activity has provided Australian law enforcement with significant insights into the operation of transnational money laundering syndicates and their connections to other serious and organised crime groups. Investigations have strengthened law enforcement's understanding of the range and extent of methods and channels used to launder funds. These include the use of the banking sector, alternative money remitters, informal value transfer systems, casinos, trade-based money laundering, online wagering platforms, high-value commodity trading, complex domestic and international business structures, securities markets, virtual currencies and professional facilitators. Money laundering continues to be a focus of law enforcement with work being undertaken across multiple government agencies and across national and international jurisdictions.

Money laundering remains a key risk to Australia and is the common element in almost all serious and organised crime. Money laundering enables criminals to hide and accumulate wealth, avoid prosecution, evade taxes, increase profits through re-investment, and fund further criminal activity. Money laundering activities also have the potential to undermine the stability of financial institutions and systems, discourage foreign investment and alter international capital flows.

11 Eligo commenced in December 2012 under the then ACC to tackle the high-risk alternative remittance sector and operators of other informal value transfer systems impacting on Australia. Eligo was extended in 2014 under the Eligo 2 National Task Force (Eligo 2) to disrupt high-priority international and domestic money-laundering operators. The task force comprised members of the ACC, AFP and AUSTRAC, with support from Commonwealth, state and territory partners, along with a number of international partners. Eligo 2 ceased on 31 Dec 2016, with work continuing under the Targeting Criminal Wealth Determination.

## MONEY LAUNDERING METHODS: MOVEMENT OF FUNDS OVERSEAS




## SPORTS BETTING

Several international organised crime groups are direct owners of online bookmakers. Multiple opportunities exist for domestic and international criminals to utilise online bookmakers to launder proceeds of crime and profit from the corruption of sporting and racing events. This includes the capacity to bet large amounts of money anonymously through offshore bookmakers.

Bookmakers operating online wagering platforms are increasingly basing their operations in jurisdictions where regulation and oversight of gambling activities ranges from minimal to completely absent. Online bookmakers offer a vast array of wagering products on sport and racing events to a global customer base, including gamblers in Australia. The capacity of Australian regulatory agencies to effectively monitor gambling through domestic licensing and regulatory arrangements has been significantly impacted by the shift to the online domain.

As at 31 December 2016, there were approximately 25.4 million mobile handset subscribers and 13.5 million internet subscribers in Australia. This is an increase of 4.7 per cent in internet subscribers since the end of December 2015.

# TECHNOLOGY

Increasingly, criminal activities are committed with the assistance of technology either via the online environment or through advances in technological capabilities, such as secure communications.[12] The online environment enables crime to be committed remotely and with relative anonymity—characteristics that are attractive to serious and organised crime groups and other motivated individuals, making the identification and prosecution of offenders more difficult. The commercial availability of secure communication platforms and surveillance equipment—such as tracking devices—provides serious and organised crime groups with the means to conceal their criminal activities from law enforcement. Serious and organised crime groups also engage the services of professional facilitators with relevant information and communication technology (ICT) knowledge and skills to assist in the commission of technology enabled crimes.[13]

In 2016, the Australian Cybercrime Online Reporting Network (ACORN) received 46,957 reports. The top three crimes reported related to scams and/or fraud (50 per cent), purchase or sale (20 per cent) and cyberbullying (7.5 per cent), and the top three modes of contact used to conduct these crimes were email, social networking and website advertising.

The majority of serious and organised crime activities are enabled, to some extent, by the use of technology. Technology is attractive to criminals as it can provide anonymity, obfuscate activities and locations, and increase their global reach by connecting them to potential victims and information around the world. Using technology to commit crime is also significantly more efficient and less resource intensive than traditional methods of perpetrating crime.

Identity crime, where personal identifying information is stolen and sold online, relies heavily on technology. Virtual currencies are used by criminals for money laundering and in exchange for illicit goods. Alternative banking services that are based online are being exploited by serious and organised crime to launder illicit funds, evade tax obligations and avoid regulatory oversight. Tax fraud has occurred as a result of compromised payroll systems and superannuation platforms have been targeted for fraud and theft. Technology is fundamental to the success of card fraud and facilitates the distribution of child exploitation material worldwide.

The two key enabling technologies currently used to facilitate serious and organised crime are virtual currencies and encryption. Virtual currencies, such as bitcoin, are increasingly being used by serious and organised crime groups as they are a form of currency that can be sold anonymously online, without reliance on a central bank or financial institution to facilitate transactions. Darknet[14] marketplaces such as Silk Road 3.0 and Valhalla

12 Secure communications include but are not limited to communication devices with military grade encryption, remote wipe capabilities, duress passwords and secure cloud-based services.

13 The Australian Cybercrime Online Reporting Network (ACORN) is a national policing initiative of Commonwealth, state and territory governments. It is a national online system that allows the public to securely report instances of cybercrime. It also provides advice to help people recognise and avoid common types of cybercrime.

14 The darknet is a routed allocation of internet protocol address space that is not discoverable by usual means. The term can refer to a single private network or to the collective portion of internet address space that has been configured in that manner. Popular darknets include Tor (the onion router), Freenet and I2P. Such networks are decentralised, routing traffic through a widespread system of servers, making it difficult to trace communications.

Marketplace are used to facilitate the sale and trafficking of illicit drugs, firearms, precursor chemicals and child exploitation materials. Australia's use of darknet marketplaces is expected to grow, given the increasing popularity of online trading and the perceived anonymity such marketplaces provide.

High-end encrypted smartphones continue to be preferred by serious and organised crime groups to reduce visibility of their activities to law enforcement. Multiple OMCGs and other serious and organised crime groups use encrypted communication devices and software applications such as Phantom Secure BlackBerry and Wickr as their primary means of communication, due to the content protection features available on these devices and applications.

Increased availability and ongoing advancement of technology will continue to provide criminals with a diverse range of resources to conduct criminal activity and impede law enforcement investigations.

## PROFESSIONAL FACILITATORS

Serious and organised crime groups engage the services of professional facilitators to launder the proceeds of crime, conceal illicit wealth and enhance their criminal activities. Professional facilitators are individuals who possess specialist skills and knowledge and who are used, wittingly or unwittingly, to facilitate criminal activities. The most common professions exploited by organised crime include lawyers, accountants, financial and tax advisers, registered migration agents, stockbrokers, real estate agents and customs brokers. Information and communications technology professionals are also emerging as a key group of professional facilitators.

As seen with the release of the so called Panama Papers in April 2016,[15] criminal groups may employ offshore service providers to conceal their illicit funds. Service providers facilitate the creation of offshore company structures and associated bank accounts, and provide administration services, nominee directors or shareholders. These providers and the activities they undertake can be legal; however, their services can also enable criminals to conceal the beneficial ownership of assets and the transfer of illicit value between jurisdictions.

Professional facilitators possess detailed knowledge of often complex areas of expertise, improving a criminal group's resilience to law enforcement detection and intervention and increasing their opportunity for success. The use of professional facilitators often results in financial gains for criminals through tax evasion, money laundering, superannuation fraud, and phoenixing activities.

## IDENTITY CRIME

Identity crime continues to be one of the most common types of crime committed in Australia, and acts as an enabler of significant criminal activities including money laundering, financial crimes, drug trafficking and fraud. The true extent of identity crime is difficult to quantify due to under-reporting, discrepancies in cross-jurisdictional reporting, and instances where identify theft is undetected. There is a growing trend towards the commission of identity crime online through the production and sale of identity documentation and fraudulent use of personal identifying information.

Identity crime commonly occurs through:

- 'phishing' activities where personal information is elicited over the telephone or internet and disclosed to a business-type entity that appears legitimate
- hacking online accounts
- retrieving personal information available on social media
- illegal access of personal information stored on business databases.

The cost of identity crime in Australia is estimated at A$2.2 billion, with prevention and response activities costing a further A$390 million.

The incidence of identity crime continues to exceed that of other personal and household thefts. 2016 AIC survey data indicates approximately 8.5 per cent of respondents had experienced misuse of their personal information and 5 per cent of all respondents reported a financial loss as a result of this misuse. Data breaches increased by approximately 5 per cent in 2015–16, with 123 voluntary and mandatory notifications reported.[16] Timely disclosure of data breaches is critical, as identity misuse typically occurs within 72 hours following the breach.

15 In April 2016, 11.5 million documents were leaked from the Panamanian law firm, Mossack Fonseca, exposing how secretive offshore tax regimes can be exploited to hide money and evade tax. See *Revenue and taxation fraud* for further information.

16 A voluntary data breach notification scheme allows businesses and agencies to self-report possible privacy breaches. Mandatory data breach notifications specifically refer to breaches of the *My Health Records Act 2012.*

Identity credentials, whether stolen or fraudulent, command high prices. Australian passports reportedly cost up to A$5,200 on the illicit online market; drivers licences and Medicare cards—the most frequently used credentials in identity crime—can be purchased for A$400 and A$250 respectively.

Compromise of one type of identity credential can often enable further compromise of other credentials. For example, unauthorised mobile phone porting—where mobile numbers are transferred to another carrier without the owner's consent—is likely to involve an earlier compromise of an identity credential such as a drivers licence.

The financial impact of identity misuse on the individual varies; however, the process of restoring identity can be both time-consuming and complex. The minor financial loss contributes to under-reporting of incidents: victims commonly report identity misuse to financial institutions, for reimbursement purposes, but not to law enforcement. Collaborative work between government, business and community sectors will help mitigate the risk of identity crime. Increasing uptake of the Document Verification Service,[17] particularly in the private sector, and use of biometric identification will strengthen identity protection.

The Document Verification Service uses name-based checks to help prevent the use of fictitious identities. It is not designed to detect instances where criminals steal information used on legitimately issued evidence-of-identity documents and substitute their own photos. To address this risk, the Australian Government is implementing the Face Verification Service, which uses photos on evidence-of-identity documents to help verify a person's identity.

It is expected the threat of identity crime will continue to evolve, particularly as the amount of personal information posted online through social, business and consumer platforms continues to grow.

## PUBLIC SECTOR CORRUPTION

Public sector corruption is the misuse of public power or position for personal and/or third-party gain or advantage. Exploitation of the public sector by serious and organised crime weakens the instruments of government and strengthens criminal networks, undermining public confidence in government and public office. There is currently limited evidence of serious and organised crime involvement in public sector corruption in Australia. Areas of the public sector considered most at risk of corruption by serious and organised crime include procurement across all levels of government, frontline agencies, and new agencies without established anti-corruption practices.

While Australia is viewed as one of the least corrupt countries, the Transparency International *Corruption Perceptions Index* has rated Australia 13th in 2016, after rating Australia 7th in 2012. Various reasons for the decline in Australia's perception ranking have been cited, including a number of well-publicised instances of corruption in sport as well as publicity generated by several recent anti-corruption agency and royal commission investigations into criminality and workplace misconduct.

17 The Document Verification Service is one of the key initiatives of the Council of Australian Governments' *National Identity Security Strategy*. It is a national online system that allows organisations to use information taken from a person's identity document, with their consent, and compare this against the corresponding records of the document issuing agency.

# VIOLENCE AND INTIMIDATION

Violence and intimidation continues to enable serious and organised criminal activity in Australia. The majority of violence involving organised crime occurs between criminal groups, rather than being directed at members of the general public. Serious and organised criminals will often use violence and intimidation to extort significant financial gain from individuals and their businesses, or to coerce them into facilitating and/or undertaking criminal activities on behalf of the organised crime group. Violence may also be used as a means to control drug networks and settle disputes with the intention of causing serious injury or death. The threat of violence posed by serious and organised crime groups is realised across all jurisdictions. For example, in 2016 a series of execution-style shootings left eight people dead in New South Wales, including a significant underworld figure who was shot multiple times on a residential street in Earlwood in Sydney.

Victims of violence and intimidation at the hands of individuals associated with serious and organised crime groups may be reluctant to report their experiences to police or health professionals for fear of retribution. Under-reporting creates challenges for determining the exact nature and extent of harm caused through the use of violence and intimidation tactics by serious and organised crime.

# ILLICIT COMMODITIES

## DRUG MARKET SUMMARY

The Australian illicit drug market remains highly lucrative, with growing demand for a wide variety of substances. Poly-drug use[18] remains a feature of the market, with some serious and organised crime groups capitalising on the demand for multiple drug types by importing, cultivating, manufacturing and/or trafficking several drug types simultaneously. These enterprises may also extend their activities to include illegal tobacco imports and firearms. Serious and organised crime plays a fundamental role in the manufacture, cultivation, importation and distribution of illicit drugs in Australia.[19]

The Australian illicit drug market is best seen as a component of the global market. The internet and darknet have enabled the rapid expansion of the global drug market, with users able to access drugs, information about availability and purity of new drugs, and manufacturing manuals online. This has meant that trends in drug use observed in Europe, Canada and the United States (those markets most similar to the Australian market) are now very quickly replicated in Australia. Fentanyl usage has been widely reported as an emerging trend overseas and has been recently observed in Australia. Increased cocaine supply and use in the United States is predicted and may have flow-on effects in Australia.

The National Wastewater Drug Monitoring Program (NWDMP) recently implemented in Australia provides a data source additional to traditional collection methods to better understand the current picture of drug usage within the Australian community. The findings of the NWDMP in combination with the assessment of drug markets drawn from the ACIC's *Illicit Drug Data Report* provide an informed picture of drug use in Australia.

Cannabis remains the most commonly used illicit drug in Australia. However, the ACIC assesses that the methylamphetamine market poses the highest level of risk to Australia. Since the decline in heroin use in the early 2000s, the Australian drug market has generally been poly-drug, stimulant-based. This has been most evident in recent years, with the rising use of methylamphetamine, particularly crystal methylamphetamine (ice). China continues to be a major embarkation point for methylamphetamine imported into Australia, with Canada and South-East Asia also noted as key embarkation points.

## METHYLAMPHETAMINE

Australian urban and rural environments are affected by methylamphetamine use and associated harms. Wastewater analysis confirms methylamphetamine as the illicit drug consumed at highest levels tested across all regions in Australia.[20] Comparable levels of consumption were identified between regional and capital cities in Australia, with the exception of South Australia, where the state capital recorded higher levels. Western Australia recorded the highest consumption levels, with both regional and capital sites exceeding the national average.

18 Poly-drug use refers to the use of two or more illicit drugs in combination to achieve a particular effect.
19 This report is not intended to provide a comprehensive picture of Australian illicit drug markets. Detailed overviews of each of the Australian illicit drug markets can be found in the ACIC's *Illicit Drug Data Report*.
20 Wastewater analysis undertaken as part of the NWDMP does not test for cannabis consumption apart from the synthetic cannabinoids JWH-073 and JWH-018.

The market in Australia has traditionally been supplied by domestically produced methylamphetamine; however, in the last few years there has been an increase in importations of finished product, to the extent that imported product has now overtaken the amount of product from domestic manufacture. The use and distribution of methylamphetamine in Australia (particularly crystal methylamphetamine) has grown rapidly in the last seven years. Since 2013, crystal methylamphetamine has been the dominant form.

## CASE STUDY: LARGE-SCALE IMPORTATION OF METHYLAMPHETAMINE

In March 2017, a joint operation by the AFP and the Australian Border Force (ABF) resulted in the seizure of 540 kilograms of methylamphetamine concealed within 396 bottles labelled as protein powder. The street value of the seizure is estimated at approximately A$324 million. Eight people were arrested, with subsequent search warrants executed in Western Sydney locating an additional five kilograms of methylamphetamine, small amounts of cocaine and ecstasy, five firearms, ammunition and a further A$35,000 in cash.

Serious and organised crime groups are deeply entrenched in the importation, manufacture and distribution of methylamphetamine in Australia, with two-thirds of targets on the National Criminal Target List reportedly involved in the sale and distribution of methylamphetamine and/or its precursors. These figures include members of OMCGs as well as domestic and transnational serious and organised crime groups. Many groups that previously operated in isolation now work collaboratively to access broader distribution networks and ultimately maximise profits. Serious and organised crime groups also seek access to legitimate industry to enhance or conceal their activities. The transport sector, licensed premises, the security industry and the chemical industry are targets for infiltration and exploitation by participants in the methylamphetamine market.

## PRECURSOR CHEMICALS

Precursor chemicals are essential for illicit drug production. Every gram of drug manufactured or reconstituted in Australia relies on the diversion of a precursor, pre-precursor, reagent or solvent from legitimate distribution channels within Australia, or the illegal importation of these products. The strong demand for illicit drugs and the significant profits to be made from the sale of precursor chemicals have made this a profitable enterprise in itself. The most prevalent and sought-after precursor chemicals include those used in the manufacture of:

- methylamphetamine—such as ephedrine, pseudoephedrine and phenyl-2-propanone (P2P)
- 3,4-methylenedioxyamphetamine (MDA) and 3,4-methylenedioxymethamphetamine (MDMA)—such as helional, safrole and 3,4-methylenedioxyphenyl-2-propanone (MDP2P)
- gamma-hydroxybutyrate (GHB)—such as gamma-butyrolactone (GBL) and 1,4-butanediol (1,4-BD)
- lysergic acid diethylamide (LSD)—such as ergometrine and ergotamine
- substances used in the reconstitution of steroids into injectable forms—such as benzyl alcohol and benzyl benzoate.

The largest proportion of the market is composed of precursors for the manufacture of methylamphetamine, which remains the predominant drug produced in clandestine laboratories detected nationally. Since 2014–15, there has been an increase observed in importations of finished product (methylamphetamine) and a decrease in the number of detected importations of precursors. More recently, however, the size and sophistication of amphetamine-type stimulant laboratories has increased, as has the size of detected precursor importations. This trend may be indicative of a change in precursor importation and diversion methodologies. Residential areas remain the primary location for clandestine laboratories in Australia, with the residual contamination arising from illicit drug manufacture presenting a serious risk to the community and the environment. Clandestine laboratories remain an ongoing threat in rural and regional centres.

Precursor chemicals can be diverted from a range of sources, including the legitimate chemical industry, the transportation and logistics industry, medical facilities and pharmacies. Serious and organised crime groups have attempted to infiltrate these industries. They may also establish companies to give the appearance of legitimacy to precursor importations. Serious and organised crime groups are very resilient and adaptable to shifts in precursor availability, employing 'cooks'[21] who can create precursors, such as ephedrine, in clandestine laboratories or who are able to develop new manufacturing methods which do not require access to controlled chemicals.

## COCAINE

The majority of the world's cocaine is produced in Peru, Bolivia and Colombia. Cocaine is imported into Australia by a diverse range of transnational organised crime groups.

In comparison to markets in North America and parts of Europe the cocaine market in Australia is lucrative but small. In Australia, cocaine use tends to be concentrated in the eastern seaboard states, where there appears to be greater availability. The findings of the NWDMP confirm cocaine consumption in capital city sites in New South Wales to be well above the national averages. Consumption is typically higher in capital city sites, with many regional sites showing minimal levels of cocaine consumption. User surveys such as the *Illicit Drug Reporting System* and the *Ecstasy and Related Drugs Reporting System* also indicate varying degrees of cocaine availability in all states and territories.

There were several large detections of cocaine in late 2016, indicating a possible expansion of the market. These detections, and another significant seizure in early 2017, all involved the use of sea vessels. As outlined in the case study below, the total weight of the seizures was 3.3 tonnes. Significantly, the seized cocaine was transported on vessels originating from North, South and Central America and China, emphasising the international diversity of the cocaine threat to Australia.

21 'Cook' is a term used to describe a person who manufactures amphetamine-type stimulants.

## CASE STUDY: ATTEMPTED LARGE IMPORTATIONS OF COCAINE ON BOARD SEA VESSELS

- In August 2016, a joint operation between the ABF, the AFP, the United States Homeland Security Investigations, the New Zealand Customs Service and the Canada Border Services Agency resulted in the seizure of approximately **95 kilograms of cocaine** from a cruise ship in Sydney.
- On 12 December 2016, a commercial vessel was intercepted; approximately **186 kilograms of cocaine** was seized from the vessel.
- An international multi-agency operation involving the AFP, the ABF and New South Wales Police Force resulted in the seizure on 25 December 2016 of approximately **500 kilograms** of cocaine in New South Wales, and an earlier seizure in March 2016 of more than **600 kilograms** of cocaine in Tahiti which was allegedly destined for Australia.
- In February 2017, an AFP investigation supported by the New Zealand Customs Service, the Organised Financial Crime Agency of New Zealand, the Fijian Transnational Crime Unit, French Polynesian authorities and the ABF resulted in the seizure of more than **1.4 tonnes of cocaine** on board a yacht.

Between 2013 and 2015, Colombia experienced the two largest single-year coca cultivation increases ever recorded. As a result, it is predicted that in 2017 the United States will very likely experience the highest cocaine supply and use levels in a decade. It is possible that these high yields may account for the large detection of cocaine in Australia in 2016, and that Australia may see a growth in cocaine supply and a corresponding increase in the domestic market for cocaine in Australia.

## MDMA

Wastewater analysis indicates MDMA consumption levels are relatively low across the country, with minimal differences identified between regional and capital city sites. In recent times, however, there has been an increase in MDMA production, most notably in the Netherlands, Belgium and Germany. This has had a flow-on effect felt across the world, with some large importations detected in Australia. Although importation remains the primary source of supply to the Australian market, some manufacture does occur domestically. While the number of MDMA laboratories detected nationally remains low, there was a sixfold increase in detections, from three MDMA laboratories detected in 2013–14 to 18 in 2014–15.

MDMA is also commonly known as 'ecstasy', although not all drugs sold as ecstasy in Australia actually contain MDMA. Forensic analysis of ecstasy tablets, capsules, powder and crystals reveals that some contain a mix of MDMA and other drugs such as methylamphetamine, or contain a mix of licit and illicit substances with no MDMA. There have also been instances where no illicit substances have been detected. Genuine MDMA remains a highly desirable drug for users, and is often incorrectly perceived as a 'safe' alternative to other stimulants. There is potential for a large and lucrative market for MDMA to re-develop in Australia, driven by a strong user base.

## CANNABIS

Cannabis is the most commonly used illicit drug in Australia. Almost all cannabis consumed in Australia is cultivated domestically, with the majority of border detections being of cannabis seed. Cannabis cultivation occurs in all Australian states and territories, and includes indoor hydroponic cultivation as well as outdoor 'bush' cultivation. Recent user surveys rate cannabis as 'very easy' to obtain, with hydroponic cannabis viewed as having high potency and bush cannabis as having medium potency.

Serious and organised crime groups are well established in the Australian cannabis market, which is robust and profitable. There is considerable diversity in the size and sophistication of cannabis cultivation in Australia, from small-scale cultivation for personal use through to large indoor hydroponic or outdoor crops. In many cases, those involved in indoor hydroponic cultivation are assisted by professional facilitators in the real estate industry and electrical trades. Association with the hydroponics industry provides criminals with easy access to equipment and fertilisers.

The crop cycle for hydroponic cannabis crops is short, making cannabis a popular choice for groups seeking to raise revenue quickly. Serious and organised crime groups are increasingly using cannabis cultivation as part of their business model, setting up multiple crop houses simultaneously to generate funds to reinvest into other criminal activities including the importation of methylamphetamine.

## HEROIN

The majority of the world's illicit opium poppy cultivation occurs in South-East Asia, South-West Asia and South America. Afghanistan, in South-West Asia, is the leading cultivator and producer of opium globally. Drug profiling data indicates the majority of analysed heroin seizures in Australia originate from South-East Asia, with fluctuating supply originating in South-West Asia. Serious and organised crime is entrenched in the market, and a range of groups are involved in the importation and distribution of heroin in Australia.

There are inconsistent indicators of change occurring in the heroin market at present. The number and weight of border detections of heroin decreased in 2015–16, but there were also several short-term spikes in overdoses in some states throughout 2016. It is unclear if these were due to the natural ebb and flow of the market, or to longer-term change. It is possible that changes in the market may also be attributable to opioid users moving between pharmaceutical opioids and heroin, due to the similar effects, and to the tendency for users to switch between commodities depending on availability.

## ILLICIT PHARMACEUTICALS

The illicit pharmaceutical opioid market is inextricably linked to the heroin market because of the similarities in the effects of these substances on the user. Pharmaceuticals commonly misused include opioid-based pain relief medications, opioid substitution therapies, benzodiazepines and codeine. The synthetic opioid fentanyl is an emerging drug of choice globally. Fentanyl, carfentanil and other potent illicit pharmaceuticals such as W-18 have been detected in Australia and are available on the darknet. The strength of pharmaceutical opioids such as fentanyl—estimated to be 80–100 times more potent than morphine—presents significant health risks if misused.

## CASE STUDY: USE OF INTERNATIONAL MAIL STREAM TO IMPORT ILLICIT PHARMACEUTICALS

The Australian Border Force have seized more than 50 packages of fentanyl in the past five years, the majority of which have been imported into Australia through the international mail stream. Importation of the drug W-18 via the international airmail system has also been detected in recent years. W-18 is claimed to have been responsible for overdoses among users who believed they were taking fentanyl.

A key source of illicit pharmaceuticals continues to be diversion from legitimate medical use. This causes significant financial cost to the government when drugs diverted are also subsidised on the Pharmaceutical Benefits Scheme.[22] Anecdotal evidence suggests the use of illicit pharmaceuticals is high in rural and remote communities, where access to illicit drugs may be limited. Recent findings of the NWDMP indicate consumption of both fentanyl and oxycodone is higher in most regional sites than in capital city sites. Fentanyl use was particularly high in regional sites in New South Wales, South Australia, Queensland and Western Australia. Data collection on fentanyl consumption in Adelaide indicates consumption has been relatively constant over a four-year period (2013–16), with the exception of a spike in 2015. It is unclear whether these results are indicative of misuse of pharmaceuticals in regional areas or reflect prescribing habits of medical professionals. Organised crime involvement in fentanyl distribution is currently unknown.

## TRYPTAMINES

Tryptamines are hallucinogenic substances that act on the central nervous system, distorting mood, thought and perception. In Australia, the most commonly used tryptamines remain lysergic acid diethylamide (LSD), psilocybin-containing mushrooms ('magic mushrooms') and dimethyltryptamine (DMT). Recent years have also seen the emergence of a range of hallucinogenic substances that mimic the effect of these substances; these are known as new psychoactive substances (NPS) and are discussed in the next section.

Tryptamine users are active on social media, contributing to forums and websites to share experiences and to source substances. Commentary on social media can range from basic chatter to detailed instructions on use, dosage and side effects. Tryptamine use has long been associated with spiritual and/or religious rituals, and regular users have forums dedicated to promoting it.

LSD is predominantly self-sourced over the internet. Similarly, psilocybin-containing mushrooms are generally obtained for personal use or supplied in close circles. The internet continues to have a role in both supply and promotion of tryptamine use.

22 The Pharmaceutical Benefits Scheme is a federally funded government program that subsidises the cost of a broad range of medicines.

# NEW PSYCHOACTIVE SUBSTANCES

New psychoactive substances[23] are synthetically created substances that have a similar chemical structure to an illicit drug, or mimic its effects. Often referred to as 'legal' alternatives[24] to illicit substances, NPS comprise a range of substances, including stimulants, hallucinogens, anaesthetics and cannabimimetics, also known as synthetic cannabinoids. Illegal synthetic drugs and cannabinoids have previously been detected for sale as 'legal highs' at retail outlets under various product names.

There continues to be an increasing range of NPS manufactured and distributed internationally. At the end of 2015, the United Nations Office on Drugs and Crime reported 644 different substances in the global market.

NPS have been available in the Australian market since the mid-2000s and have increased in availability and popularity in recent years. The NPS market is highly reactive, appearing to increase and decrease in response to changes in other drug markets. The darknet is used extensively as a medium for sales of NPS, as well as for information sharing and social commentary on these substances.

Survey data indicates the use of synthetic cannabinoids dropped from 16 per cent in 2013 to 4 per cent in 2016. It is believed the decline in use of synthetic cannabinoids is related to users' negative reports about both the high and the comedown following use of the substances.

Although detection methods for measuring the cannabinoids JWH-018 and JWH-073 were included in the NWDMP, neither compound was detected in any of the analysed samples. Detections of methylone and mephedrone were measured through the parent compound; while the substances were detected at a series of sites across the country, the level of consumption was considered low. Historical data on methylone and mephedrone detections in Adelaide indicates consumption of both these substances has steadily declined over the last six years. These findings corroborate the assessment that the NPS market—composed of some potentially lethal substances—is very small relative to the more traditional drug markets.

# ANAESTHETICS

The two anaesthetics most commonly diverted for illicit use in Australia are ketamine hydrochloride (ketamine) and gamma-hydroxybutyrate (GHB), also known as 'fantasy', 'juice', 'lucy' or 'G'. Both substances have well-established, albeit small, niche markets, primarily consisting of users based in capital cities along the eastern seaboard. There are indications drug users seeking alternatives to MDMA may turn to anaesthetics during periods of reduced MDMA availability.

23 NPS are also known as novel substances, novel psychotropic substances, emerging psychoactive substances, analogues, mimetics, legal highs, new synthetics, synthetics, herbal highs or designer drugs. The term does not necessarily refer to a new invention, as many NPS may have been synthesised years or decades ago, but rather that they have recently emerged on the market.

24 Use of the term 'legal' may not reflect the true legal status of these substances under Australian law.

Legitimately used as a medical or veterinary anaesthetic, ketamine is also used illicitly for its sedative and hallucinogenic effect. It is frequently detected as an adulterant in tablets sold as ecstasy. Serious and organised crime has not been identified as playing a key role in the ketamine market in Australia. Ketamine tends to be diverted or imported into the Australian illicit market in relatively small quantities, reflecting personal use or small-scale distribution.

GHB is a powerful central nervous system depressant readily manufactured from its precursors, gamma-butyrolactone (GBL) and 1,4-butanediol (1,4-BD). GBL and 1,4-BD have legitimate uses as solvents in industrial chemical processes, including in the production of polymers. If ingested, both GBL and 1,4-BD metabolise into GHB in the body. The effects of GHB vary greatly depending on the dose, and even a very small increase in dose can lead to overdose.

There are elements of organised crime present in the Australian GHB, GBL and 1,4-BD markets, with some transnational organised crime groups implicated in importations into Australia and other groups being involved in domestic manufacture and trafficking. The level of sophistication required to operate in this market is quite low, given the ease with which GBL and 1,4-BD can be diverted from legitimate supplies.

## PERFORMANCE AND IMAGE ENHANCING DRUGS

The performance and image enhancing drugs (PIEDs) market in Australia is growing rapidly, consisting of users from an increasingly diverse demographic using a wide range of substances. One of the key drivers of the market is a strong youth culture that is focused on achieving a muscular and athletic physical appearance, particularly prevalent among young men.

The use of PIEDs has also been associated with violent behaviour, particularly among young men using PIEDs in conjunction with alcohol and/or other illicit drugs. This has influenced legislative changes in several jurisdictions, resulting in increased penalties for the unlawful possession of steroids.

Serious and organised crime groups are involved in the importation, manufacture and distribution of PIEDs in Australia. However, individuals also import PIEDs for personal use or for supply to friends and acquaintances. A significant number of PIEDs have been detected in the mail. There have been multiple detections of large commercial clandestine PIEDs laboratories in recent years. These laboratories often involve the reconstitution of powdered steroids into an injectable form.

## ILLICIT TOBACCO

Serious and organised crime remains entrenched in the illegal tobacco market, both through the illegal importation of tobacco products and through the local production of illegal tobacco. Source countries for illicit tobacco include the United Arab Emirates, Malaysia, Indonesia and Singapore.

Between October 2015 and December 2016, the ABF Tobacco Strike Team seized more than 22 tonnes of tobacco and 52 million cigarettes. Theses figures include the discovery of 18 million sticks of 'Napoli' brand cigarettes in a container arriving from China on 3 December 2016. The street value of this discovery is estimated at more than A$5 million with the total amount of duty evaded estimated at A$11 million. A further five million illegal cigarettes and one tonne of loose leaf tobacco were detected by ABF officials at the International Mail Centre in January 2017.

The local production of illegal tobacco is an enduring problem. The Australian Taxation Office (ATO), in collaboration with law enforcement partners, continues to make significant seizures across several jurisdictions. In March 2017, an illegal tobacco crop worth more than A$11 million was discovered in New South Wales. This seizure followed similar searches in Victoria and New South Wales in late 2016 and early 2017 netting illegal tobacco with a potential excise value greater than A$10 million. This highlights the significant profits to be made from the illegal tobacco market in Australia.

## ILLICIT FIREARMS

The use and distribution of illegal firearms poses a serious threat and safety concern to the Australian community. Firearms are used by a wide range of criminals to protect their interests, for intimidation through the threat of harm, or to commit acts of physical violence. Reporting indicates several serious and organised crime groups are involved in trafficking firearms. No single group dominates the sale and supply of illicit firearms to the Australian market.

The extent of the illegal firearm market in Australia remains difficult to estimate. The ACIC conservatively estimates there are approximately 260,000 firearms in the domestic illicit market, including 250,000 long-arms and 10,000 handguns. Historically, diversion of firearms to the illicit market was primarily through the grey market.[25] Recent trends in diversion methods include theft, domestic manufacture, and illegal importation.

The ACIC Firearm Trace Program (FTP) data for 2015–2016 revealed theft as the primary diversion method, accounting for 8.5 per cent of firearms traced.[26] Firearm theft is often not contemporaneous with detection and could have occurred years before the firearm was actually located. Regional or isolated locations are particularly vulnerable to firearm theft, such as hobby farms characterised by long periods of absence or safe storage areas located away from main dwellings. The sophisticated and organised theft of firearms from licensed dealers is rare, but can greatly increase the number of illegal firearms in the illicit market, as indicated by the theft of 130 handguns from a well-established firearms dealer in Western Australia in March 2017.

25 The grey market consists of illegally held long-arms that were not registered or surrendered under the 1996 *National Firearms Agreement*.

26 The ACIC Firearm Trace Program provides a national picture of illicit firearms located by law enforcement agencies. Since submissions of trace requests by law enforcement to the FTP are voluntary, FTP statistics do not reflect the total number of illicit firearms located in Australia.

Domestic manufacture of illicit firearms, including single-shot pen guns and handguns, key ring guns and submachine guns, is an enduring issue. As technology develops, increased attempts to produce reliable illicit firearms have been observed. The online environment provides a source of firearm manufacturing plans, CNC[27] and 3D software, and techniques shared by users intent on manufacturing illicit firearms. The reliability and cost-effectiveness of 3D manufactured firearms fails to match those of factory-produced firearms.

The scale of importation of illegal firearms and components into Australia is difficult to define. FTP data for 2004–2016 indicates approximately 7 per cent of all diverted handguns were illegally imported. In 2015–2016, one per cent of all firearms traced by the FTP related to illegal importations.

Australian border detections of undeclared firearms, parts and accessories have remained stable over the last three years. The majority of undeclared firearms imports are attributed to opportunistic individual importers rather than serious and organised crime groups. Importation occurs primarily through the international mail stream, with post parcel lockers providing a further level of anonymity. Members of a New South Wales syndicate were recently convicted of importing over 130 semiautomatic handguns and firearm parts into Australia through the mail stream in 2012, and the majority of these handguns are yet to be recovered by law enforcement. Encrypted websites within the darknet that provide online platforms for the purchase of illicit commodities including firearms are likely to continue to be exploited.

27 Computer Numerical Control.

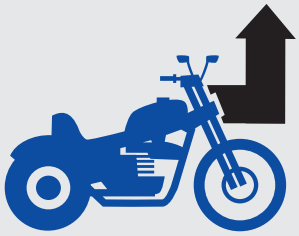
# ILLICIT FIREARMS IN AUSTRALIA

While Australia has some of the **strongest firearm controls in the world**, illicit firearms remain a **desirable commodity** and **enabler for criminal activity**.

There are more than
**250,000 long-arms**

and **10,000 handguns**

in the illicit market.



An **increasing number** of organised crime groups, including outlaw motorcycle gangs, are **trafficking illicit firearms**.

> ***One** illegal firearm in our community is **one too many.***
>
> *Chris Dawson, former ACIC CEO*

Firearms enable **organised crime groups** to be **more lethal** in their activities.

**2004–2016** ACIC received

**6,874**
**requests** for domestic firearm traces.

There are more than
**2.89 million**
**legally registered firearms**
in Australia and approximately
**816,000**
**firearm licences**.

ACIC holds more than
**1.8 million**
**historical records of firearms transactions.**

# SERIOUS FINANCIAL CRIME

## THEME SUMMARY

The ACIC has identified five key elements of financial crime:

- cybercrime
- investment and financial market fraud
- revenue and taxation fraud
- superannuation fraud
- card fraud.

Financial crimes are diverse in nature and scale, and in the level of harm they cause. The modern globalised economy and advances in technology create new opportunities for organised crime to exploit vulnerabilities for illicit profit. The expansion of serious and organised crime into the financial sector poses a significant risk to the integrity of the Australian economy, financial markets, regulatory frameworks and revenue collection. This risk is particularly salient in the current economic environment, where damage to financial markets, government revenue base and the savings of private individuals can have far-reaching implications.

Conservative estimates put the cost of organised fraud[28] to the Australian economy at A$6.3 billion between 2013 and 2014—including revenue and tax evasion, superannuation fraud, card and financial transaction fraud. The intermingling of licit and illicit financial transactions makes it difficult to fully assess the extent of financial crime in Australia. The complexity and potential scale of financial crime poses an ongoing challenge not only to law enforcement but also to regulators.

## CYBERCRIME

Cybercrime against individuals, businesses and governments can be conducted from anywhere in the world. The threat to Australia from cybercrime is transnational in nature with the majority of cybercrime affecting Australia originating from Russia and Eastern Europe. The primary threat is from temporary networks of people who collaborate but may live in geographically diverse locations. This means that cybercrime activities are inherently difficult to investigate.

Cybercrime is defined[29] as:

> crimes where computers or other information communications technologies are an integral part of an offence, such as online fraud, identity crime and the distribution of child exploitation material.

28 The cost of government support for victims, based on the approximate size of the illicit activity and the percentage of serious and organised crime involvement.
29 Australian Cyber Security Centre 2015, *ACSC 2015 Threat Report*, ACSC, Canberra, p.8.

Cybercrime is a low-risk, high-return criminal enterprise with potentially lucrative financial gains. Australia's high levels of technology use and relative wealth ensure the persistence of the cybercrime threat in Australia. The principal forms of serious and organised cybercrime affecting Australia involve ransomware, credential-harvesting malware, and distributed denial of service (DDoS) extortion. Computers and devices of private individuals and commercial entities as well as government systems are all at risk from cybercrime.

## RANSOMWARE

Ransomware is a form of malware that stops a victim from using their computer, or files, until a sum of money is paid to a cybercrime actor. It targets a victim's computer via malicious emails and websites. Once installed, ransomware encrypts the victim's files, and then directs the victim towards a webpage with instructions on how to pay a ransom for their data to be decrypted. Cybercriminals have used ransomware to demand payments from A$500 to A$3,000 (in bitcoin), with some businesses subjected to targeted attacks requesting tens of thousands of dollars. In 2016, the ransomware Cryptolocker was discovered on the computer system of an Australian government agency after an employee clicked on an Australia Post-themed email. Cryptolocker re-imaged the staff member's workstation, resulting in thousands of files stored on an associated government server being encrypted by the ransomware.
The most effective ransomware campaigns in Australia use the branding of trusted and well-known Australian corporations as part of their social engineering techniques.

Australian government organisations have also been targets of credential-harvesting emails. Such emails direct users to access a document via a shared drive that subsequently requests credentials be entered in order to access the document. Once an email account has been compromised, the contacts within the account are then sent malicious emails appearing to be from the legitimate and trusted source.

## CASE STUDY: ONGOING CYBERCRIME AGAINST FINANCIAL INSTITUTIONS

Malware continues to be used by cybercriminals to attack commercial and private enterprise. The Gozi Trojan, first discovered in 2007, is one of the longest-operating banking Trojans.

Despite three of its developers being arrested by the United States Federal Bureau of Investigation in 2013, Gozi and its various iterations continue to be used by multiple cybercriminal groups, posing a persistent threat to the financial sector. In 2016, Gozi was identified as active in Australia, Canada, Italy, Japan and Spain, amongst other nations.

In February 2016, cybercriminals fraudulently diverted US$851 million from the Bangladesh Bank. The cybercriminals infected the Bangladesh Bank's SWIFT payment system with malware that allowed them to deactivate system integrity checks, alter payment details, and suppress notification of the altered payments. While the majority of the stolen funds were recovered, US$81 million remains outstanding.

The successful theft of US$81 million highlights the significant financial rewards that can be obtained by directly targeting bank systems rather than bank customers. This has resulted in several cybercrime groups taking an increased interest in finding and exploiting vulnerable SWIFT systems. While less-developed countries have been attacked initially, Australia is also a potential target.

## CREDENTIAL-HARVESTING MALWARE

Mirai is an example of malware that is comparatively unsophisticated; the source code is readily available for use by actors at the lowest levels of sophistication. Mirai malware turns Internet of Things[30] devices into 'bots' to be used by actors for malicious purposes such as DDoS. Mirai operates by scanning the internet for a suite of devices with known default credentials, including DVRs, printers and home internet routers. It uses those credentials to install itself onto the device, and then scans the internet for new vulnerable devices to infect. Despite its relative simplicity, Mirai has been used to implement some of the largest DDoS incidents.

On 20 September 2016, the Mirai botnet launched a DDoS attack against OVH, a major web hosting company based in France. A DDoS attack was also launched against the website of an independent IT security journalist, Brian Krebs, forcing his website offline despite it being protected by one of the leading DDoS protection services, Akamai. Regardless of its relative simplicity, this attack by Mirai was considered one of the largest DDoS attacks ever seen.

## DDOS EXTORTION

DDoS extortion occurs when a specific cyber-actor threatens to launch DDoS activities against an organisation unless a fee is paid. DDoS extortion threats have been raised against small, medium and large businesses including financial institutions in Australia. The instances of DDoS extortion have increased, with threats coming from both domestic and international serious and organised criminal syndicates.

## BUSINESS EMAIL COMPROMISE

Business email compromise (BEC) is a cybercrime scheme that targets large and small businesses for financial gain. BEC can take many forms but most commonly involves impersonating a high-level employee in order to change invoice details or request immediate funds transfers. BEC requires few technical skills; most effort is spent on social engineering and research on targets.

BEC is starting to gain ground in Australia and—since the inception of ACORN in November 2014—victim reports have increased. Due to its increasing prevalence, BEC is now being quantified in Australia for the first time. Analysis of ACORN data found 749 cases reported in the 2015–16 financial year, and 243 cases reported within the first quarter of the 2016–17 financial year.

30 The Internet of Things (IoT) is made up of physical objects that have embedded network and computing elements, and communicate with other objects, or computers, over a network, usually the internet.

# INVESTMENT AND FINANCIAL MARKET FRAUD

Domestic and transnational serious and organised crime groups involved in investment and financial market fraud continue to target Australia. Online platforms and exploitation of markets are playing an increasingly important role in investment and financial market fraud, which refers to three different types of fraud:

- fraudulent investment schemes, such as boiler-room fraud and Ponzi schemes[31]
- manipulation or exploitation of the legitimate share market to artificially raise or lower the price of securities
- exploitation of financial market securities to commit fraud or to launder the proceeds of crime—for example, off-market share transfers and fraudulent share schemes.

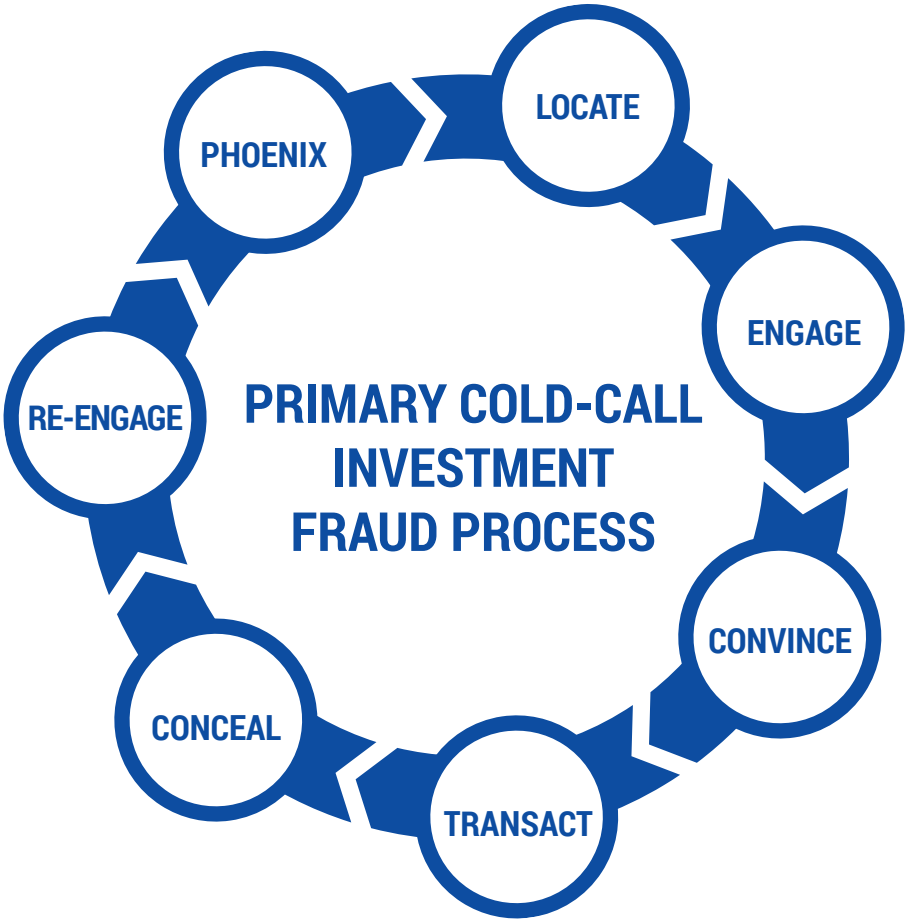
Boiler-room or cold-call investment fraud operations pose an enduring issue for law enforcement. In January 2017, a 51-year-old man was extradited from South Australia to face five counts of fraud in Queensland over his alleged involvement in multiple Gold Coast-based investment companies offering shares in products that were ultimately flawed. Approximately A$6 million was taken from unsuspecting individuals who had invested in predictive betting software that promised to provide high levels of financial returns accompanied by tax-free gains. Once delivered, the software failed to work and the organisers of the scheme refused to return the funds to investors.

The availability of computer programs that create orders to buy and sell securities has provided further opportunities for serious and organised crime groups to engage in market manipulation. These computer programs create artificial interest in a particular security by driving the price either up or down. Once this has occurred, securities that are held can be sold (at a higher price) or bought (at a lower price). Such activity is known as 'spoofing'.

## CASE STUDY: TRANSNATIONAL ELECTRONIC MARKET MANIPULATION

In mid-2015, an online share-trading account was created by an individual believed to be based in Russia. This account was used to purchase Australian-market-listed securities. The individual was also able to gain access to a number of other legitimate share-trading accounts and raise funds through the sale of shares held within them. These funds were then used to purchase shares in the same companies as those held in the recently created share-trading account, thereby pushing up the price. Once the price had increased to a certain level, the individual sold the original shares, realising a profit. In this instance, the scheme was detected and authorities were able to stop the transfer of the profits offshore.

31 A Ponzi scheme is a fraudulent investment scam where a promoter promises investors a return on investment, but this return is generated from new capital obtained from new investors rather than profit earned from legitimate sources. Operators usually entice new investors by offering higher returns than other investments. The scheme often falls apart because the promoter starts to spend the money too quickly or the pool of investors dries up.




| | |
|---|---|
| **LOCATE** | Telemarketer cold calls potential victims offering investment opportunities. |
| **ENGAGE** | Follow up contact from a sales consultant who uses an established 'script' to entice potential victims to enter into a contract with the company. |
| **CONVINCE** | Further sales techniques are employed to convince potential victims to invest, often including repeated calls and referrals to the company website that appears legitimate. |
| **TRANSACT** | The victim enters into a contract with the company and transfers funds–often between A$5,000–50,000. |
| **CONCEAL** | Invested funds are withdrawn/transferred to a separate bank account controlled by the parent syndicate. The victim's trading account may appear to be growing on the company website, but they are unable to access their investment funds. |
| **RE-ENGAGE** | The victim is re-contacted and offered upgraded investment package options to invest further funds. |
| **PHOENIX** | Company income decreases as the availability of potential victims is reduced–often a direct result of bad publicity. The parent syndicate folds the company and the scheme is re-launched under a new company name. |

# REVENUE AND TAXATION FRAUD

Revenue and taxation fraud involves the intentional abuse of the taxation system with the aim of obtaining financial benefit. It encompasses numerous non-compliant activities and can result in criminal sanctions such as fines or imprisonment. Such activities range from failing to report income in order to avoid taxation obligations to the use of complex offshore secrecy arrangements, also to evade tax. The use of professional facilitators continues to be a key enabler of revenue and taxation fraud, most notably in fraudulent phoenix activity, offshore tax evasion and the abusive use of trusts.

The Australian Taxation Office (ATO) is the principal revenue collection agency of the Australian Government and is responsible for the administration of tax products, which includes administering both income tax and the goods and services tax. In the last six months of 2016, the ATO reports tax crime investigations led to:

- 138 fraud charges
- 10 jail terms
- the seizure of illegal tobacco plants and illegal stills with a total potential excise value of more than A$18.7 million
- the execution of six search warrants relating to fraudulent phoenix activity
- the identification of attempted taxation fraud worth A$1.4 million
- the identification of false taxation claims of over A$10.8 million.

It is estimated that fraudulent phoenix activity costs the Australian economy A$3.2 billion each year. Fraudulent phoenix activity involves the deliberate liquidation of a company in order to avoid paying creditors, taxes and employee entitlements. Once a company has been liquidated, the perpetrators transfer the remaining assets to a new entity and continue to operate the same or a similar business under a new name, retaining the same ownership. The end results of phoenix activity are financial loss to suppliers due to unpaid debits; financial loss to employees through unpaid superannuation entitlements; and loss to the community due to unpaid taxation revenue.

Professional facilitators are key enablers of offshore tax evasion, as a high level of expert knowledge is required to successfully establish and operate large-scale fraud and tax evasion activities while avoiding detection. Australia-based facilitators have been seen to promote the services of offshore financial service providers. Facilitators include professionals in the import/export, accounting, legal, money remittance, finance, insurance and ICT industries. There is also evidence of superannuation and estate planning structures and strategies being part of integrated tax evasion design by private wealth groups.

Globalisation and technological advances have made it easier for individuals to hold investments in offshore financial institutions, increasing the opportunity for tax evasion. In April 2016, 11.5 million documents were leaked from the Panamanian law firm, Mossack Fonseca, exposing how secretive offshore tax regimes can be exploited to conceal wealth and evade tax. The leaked documents revealed the names of more than 1,000 Australians. Eighty of these names were matched with the ACIC's criminal intelligence holdings, and several were recorded on the National Criminal Target List.

The significance of the exploitation of offshore secrecy arrangements to evade tax is observed in recent advice provided by the ATO that, on the successful completion of Project Wickenby,[32] over $2.2 billion in tax liabilities had been raised and 46 criminal convictions secured.

While the establishment of an offshore structure or trust is often for a genuine purpose, many structures and trusts are being used to evade tax, to avoid corporate responsibility, to disguise and hide unexplained wealth, to facilitate criminal activity, and to launder the proceeds of crime. It remains difficult to identify the level of involvement by serious and organised crime in the abusive use of trusts due to the inherent complexity of the legislative and regulatory frameworks surrounding trusts and trust structures. Revenue and taxation fraud will remain a long-term issue for law enforcement as interactions between key enablers such as technology, identity crime and professional facilitators become increasingly complex and frequent.

## SUPERANNUATION FRAUD

Australia's large pool of superannuation savings continues to be an attractive target for organised crime groups. The complex nature of superannuation schemes offers a range of opportunities for fraud including the theft of contributions and fund assets, fraudulent fund investments, non-existent schemes, and excessive fees charged by advisers.

The volume of funds held in superannuation schemes in Australia is significant: over 14.8 million Australians held a super fund account as at 30 June 2016, and approximately 43 per cent of those have more than one super account.

There are various superannuation schemes available in Australia, including MySuper, retail funds, industry funds, public sector funds, corporate funds, rollover funds and self-managed super funds (SMSFs). The Australian Prudential Regulation Authority (APRA) supervises regulated superannuation funds (other than SMSFs), approved deposit funds, and pooled superannuation trusts—all of which are regulated under the *Superannuation Industry (Supervision) Act 1993.*

APRA is responsible for over A$2,198 billion in superannuation assets. APRA-regulated superannuation funds are susceptible to targeting by serious and organised crime groups: a recent increase has been observed in the use of targeted online methodologies to fraudulently access an individual's superannuation account. Superannuation funds are responding to this activity by developing data analytic capabilities designed to detect unusual or suspicious activity.

SMSFs are particularly vulnerable to incidents of fraud, in part due to the desire of individuals to source and control their own investments. At the end of the 2015–16 financial year, Australians held A$622 billion in SMSFs—a substantial and attractive pool of funds to serious and organised criminal groups.

AUSTRAC plays an important role in combating superannuation fraud, and continues to receive reports from industry on the use of fraudulent documentation in support of claims for early release of superannuation benefits or death and disability insurance payments.

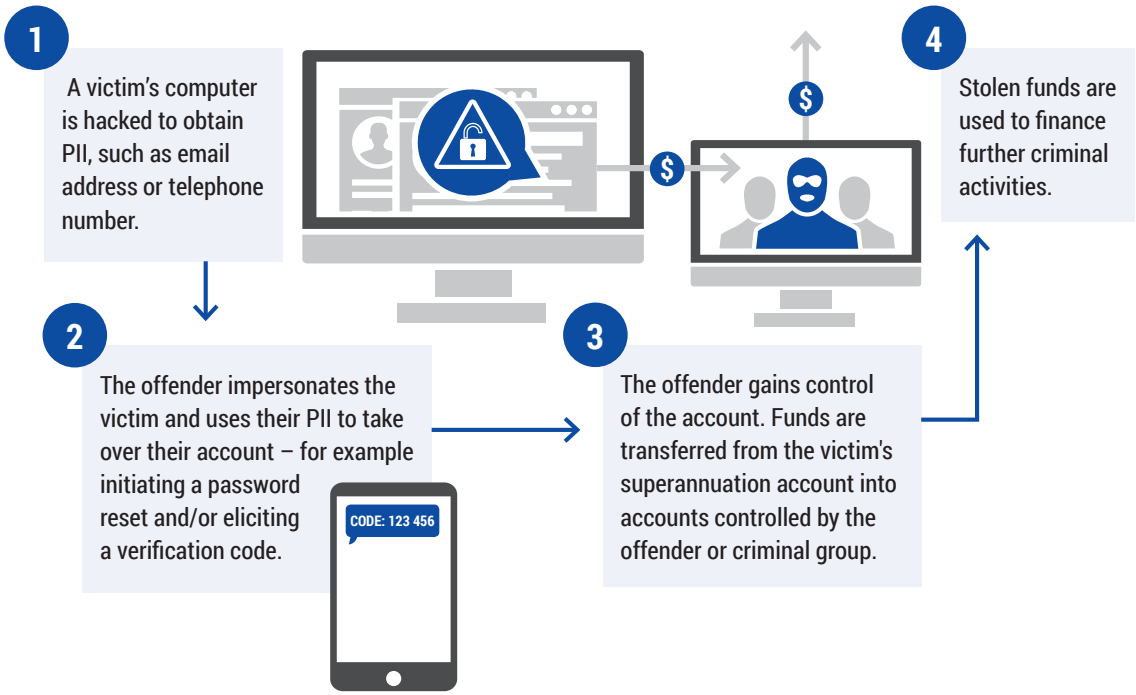
32 Project Wickenby, a cross-agency task force, was established in 2006 to protect the integrity of Australia's financial and regulatory systems by preventing people from promoting or participating in the abuse of offshore secrecy arrangements.

Individuals who have reached preservation age[33] are particularly vulnerable to theft or fraud, as funds can be transferred in and out of their account, much like a bank account. The ability to withdraw funds from a superannuation account provides an opportunity for serious and organised crime groups to access these funds if they can convince account holders to invest in a fraudulent scheme.

## CASE STUDY: PAYPAL PHISHING

In early 2017, PayPal users were targeted by a phishing campaign directing victims to fake internet pages designed to look identical to legitimate websites in an effort to steal users' login credentials and other personal information.

### HACKERS' USE OF PERSONALLY IDENTIFIABLE INFORMATION (PII) TO FRAUDULENTLY AUTHORISE FUNDS TRANSFERS




33 Access to superannuation benefits is generally restricted to members who have reached preservation age, which currently ranges from 55 to 60 years of age, depending on date of birth.

# CARD FRAUD

Card fraud is the fraudulent acquisition and/or use of debit and credit cards, or card details, and may involve:

- fraudulent applications
- theft of cards/card details
- skimming of card details at automatic teller machines
- production of fake cards
- phishing/hacking to obtain card details.

In the 2015–16 financial year, Australians spent A$703 billion on cards; A$521 million of this spending (across 2,665,806 transactions) was fraudulent. This represents a card fraud rate of 74.2 cents per A$1,000 spent, an increase from the previous 12 months (60.4 cents per A$1,000).

The Australian Payments Network (APN) attributes 77 per cent of all fraud on Australian cards to card-not-present (CNP) fraud. CNP fraud occurs when card details are fraudulently used to make purchases or other payments without the card, via phone or online shopping, betting and/or gaming platforms or other websites of a similar nature.

The introduction of chip and PIN technology has resulted in a decline in card-present fraud; however, this kind of fraud also remains a problem. In response to these new technologies, organised crime groups have altered their methodologies—for example, by uploading skimmed data to blank cards to obtain cash or to purchase high-value goods in other countries. In the 2015–16 financial year, card counterfeit and skimming fraud perpetrated in Australia and overseas on Australian-issued cards accounted for almost A$47 million.

The intersection between smartphone technology and mobile payment platforms has enabled contactless payments using smart devices containing linked credit card details. The rise in mobile payment services follows the increasing use by Australians of smartphones to make online payments and purchases and to access banking services. Vulnerabilities exist within these payment platforms that can be exploited by serious and organised crime groups via the use of malware. As Australia moves towards a cashless society, there are increased opportunities for online payment and card fraud.

# SPECIFIC CRIME MARKETS

## THEME SUMMARY

Specific crime markets include visa and migration fraud, environmental crime and intellectual property crime.

Visa and migration fraud presents a continued threat to the Australian community as well as to national security interests. Serious and organised crime groups exploit the Australian visa and migration system, engaging the services of professional facilitators to enable entry into Australia. Visa and migration fraud is highly profitable and closely linked to both identity crime and cybercrime.

Environmental crime is diverse in nature and encompasses several crime markets. Transnational organised crime syndicates and opportunistic individuals exploit these markets, which are characterised by high profit margins and low detection rates. The cost of environmental crime in the global context continues to rise, with far-reaching environmental, financial, security and social implications. Technological developments in encrypted communication and the availability of illegal online marketplaces continue to enable transnational environmental crime.

Piracy and counterfeiting are serious international issues, and many countries including Australia commit significant resources to combating them. The main forms of intellectual property crime in Australia are the importation of counterfeit goods such as clothing and the domestic manufacture of goods that infringe copyright.

## VISA AND MIGRATION FRAUD

Exploitation of Australia's visa and migration program presents an ongoing threat to Australia's border. Manipulation of Australia's visa and migration system may occur through a range of fraudulent, exploitative or non-compliant activities. These include:

- visa application fraud
- travel document fraud, including identity fraud
- visa non-compliance
- labour exploitation.

Visa and migration fraud occurs when a visa is issued on false or fraudulent grounds (visa application fraud), or when an illegitimate or illegal visa or passport is acquired (travel document fraud). Travel document fraud can also involve the fraudulent use of legitimate documents to obtain a visa or for travel. If false or fraudulent documents are used in an attempt to conceal the true identity of persons entering or leaving Australia, there is a potential impact on Australia's national security. A prominent feature in visa and migration fraud is the increasing involvement of serious and organised crime groups, who seek to exploit the Australian visa and migration system in order to facilitate criminal activities onshore.

Permanent visa fraud may occur through contrived marriages. Strategies to mitigate fraudulent partner sponsorship arrangements include a data-matching program between the Department of Human Services and the Department of Immigration and Border Protection (DIBP) to detect fake marriages, and legislative changes under the 'paying for visa sponsorship' framework.[34]

## CASE STUDY: VISA FRAUD INVOLVING CONTRIVED MARRIAGE SCAM

A registered migration agent and his wife, a marriage celebrant, were convicted in early 2017 for organising a visa scam involving 16 fake marriages between Australian women and Indian men. One witness testified to paying between A$35,000–$40,000 in fees to the migration agent and to the Australian woman he married in the scam. Both offenders received custodial sentences.

Visa non-compliance typically involves a breach of visa conditions, commonly for financial gain or to remain in Australia; it may also enable other migration threats, including labour exploitation.

Visa manipulation is a common feature of organised crime groups and businesses involved in the exploitation of labour. Visa holders may find they are exploited by such groups who employ them outside of their visa conditions with the threat of their visas being cancelled should these breaches be reported to the authorities. In June 2016, an Australian company was penalised for forcing four overseas workers, who were employed under the temporary skilled visa program, to return a portion of their fortnightly wages in cash and to work overtime without pay, while being threatened with dismissal and deportation. Taskforce Cadena was established by the Australian Government in June 2015 to target and disrupt criminals organising visa fraud, illegal work and the exploitation of foreign workers. It is a joint agency initiative between the DIBP—led by its operational arm, the ABF—and the Fair Work Ombudsman.

Significant Investor and Premium Investor visa programs present opportunities for transnational organised crime groups to launder illicit wealth. The complexity of establishing and verifying the source of funds received from offshore applicants means that a Significant Investor or Premium Investor visa may be used as a means to legitimise wealth and achieve permanent residency in Australia.

Serious and organised crime groups as well as individual actors continue to exploit vulnerabilities within the migration system to obtain entry to Australia. Migration agents may be wittingly or unwittingly utilised as professional facilitators of this activity.

Visa and migration fraud is intrinsically linked to identity crime and cybercrime, and is likely to increase in sophistication with advances in technology.

34 Civil and criminal penalties can be imposed for offering, providing or receiving a benefit in return for visa sponsorship.

## PEOPLE SMUGGLING

People smuggling is a global issue exploiting the most vulnerable of people. It can have wide ranging effects including the loss of human life, human rights abuses, threats to security and corruption. The involvement of transnational organised crime groups in people smuggling continues to grow in response to the ongoing demand for these services. Transnational organised crime groups generate significant profits facilitating the illegal movement of people. They may also use their people smuggling networks more broadly to support other criminal activities, including illicit drug and weapons trafficking as well as terrorism.

People-smuggling investigations impacting Australia involve collaboration with international partners to disrupt domestic and international organisers, facilitators and financiers. Historically, the most visible form of people smuggling to Australia occurred via the maritime stream. Operation Sovereign Borders has significantly disrupted maritime people-smuggling ventures to Australia.

# ENVIRONMENTAL CRIME

Environmental crime encompasses a diverse range of crime types including:

- illegal trade in protected flora and fauna
- illegal harvesting and trade of timber and forestry products
- pollution caused by dumping hazardous waste
- illegal trade in ozone-depleting substances
- illegal, unreported and unregulated fishing (IUU).

Environmental crime can be complex and difficult to measure, with the cost increasing on a global scale. A 2016 joint Interpol and United Nations Environment Program report[35] estimated the global annual cost of environmental crime at US$91–258 billion, an increase of 26 per cent since 2014. Assessed as the world's fourth-largest crime sector in terms of profit generation, environmental crime has far-reaching implications including the cost to future generations through the loss of natural resources and ecosystems, the loss of government revenue, the undermining of legitimate businesses, and threats to security in vulnerable regions. Criminal involvement ranges from opportunistic individuals and personal collectors of protected flora and fauna to sophisticated organised crime groups seeking to capitalise on the high profits and low detection rates.

Environmental crime in Australia is seen principally in the trade of illegal wildlife and in incidents of IUU fishing. Native vegetation clearance and water theft have previously been recognised as additional environment crime types unique to Australia. Serious organised crime involvement in environmental crime in Australia is currently unknown, with individuals and smaller networks more commonly reported. Technological developments including encrypted communications, online marketplaces and use of bitcoin currency continue to enable crime in this sector.

35 Nellemann, C; Henriksen, R; Kreilhuber, A; Stewart, D; Kotsovou, M; Raxter, P; Mrema, E; and Barrat, S. (Eds) 2016 *The Rise of Environmental Crime – A Growing Threat to Natural Resources, Peace, Development and Security*, United Nations Environment Programme and RHIPTO Rapid Response – Norwegian Center for Global Analyses, p.7.

The illegal trade of wildlife and CITES[36] products is highly profitable, estimated to cost US$7–23 billion per year globally. It is also linked to the decline of many endangered species. A domestic and transnational market currently exists within Australia, although available data on seizures is limited. The trade is bi-directional: Australian native species are in demand overseas, and there is a market for exotic species in Australia. Interest in this market from serious and organised crime groups is likely to grow, given the high profitability and increased opportunities to trade globally through encrypted communications and via the darknet.

## CASE STUDY: AUSTRALIAN MAN ARRESTED FOR ILLEGAL WILDLIFE TRAFFICKING

In March 2017, a joint operation between the AFP and the Department of Environment and Energy resulted in the arrest of a Sydney man who was charged with 41 offences relating to illegal wildlife trafficking. Investigators seized six packages destined for Sweden containing more than 40 native Australian lizards. The offender also allegedly imported 16 packages from Thailand containing over 200 animals.

Illegal, unreported and unregulated fishing is sometimes linked to other transnational organised crimes including drug trafficking, human trafficking and migrant smuggling. Incidents of IUU fishing in Australia target high-value species. Regular surveillance patrols and monitoring of Australian waters led to a significant decrease in IUU fishing apprehensions over the last decade, with 17 apprehensions in 2015–16.

## CASE STUDY: SIX TONNES OF SEA CUCUMBER SEIZED

In June 2016, two Vietnamese fishing vessels were apprehended approximately 600 kilometres north-east of Cairns, Queensland within the Coral Sea Commonwealth Marine Reserve. Approximately six tonnes of sea cucumber were located on the vessels and the 30 crew members pleaded guilty and were convicted for breaking Australian fisheries and environmental laws. Penalties included suspended jail sentences ranging from two months for the crew members to five and seven months for the masters of the vessels. The two fishing vessels operated by the convicted illegal fishermen were confiscated by the Australian Fisheries Management Authority and destroyed in Cairns.

Significant increases in the global cost of environmental crime were identified within the illegal harvesting and trade of timber sector. The majority of this crime type is trade-related, characterised by practices such as under-reporting of export volumes, tax evasion, bribery, and altering of species names to co-mingle legal and illegal commodities.

36 Convention on International Trade in Endangered Species of Wild Fauna and Flora.

Australia is primarily a destination country for illegal timber, with previous estimates suggesting up to 10 per cent of imported products contain illegal timber. Reporting indicates small-scale illegal logging was occurring within the Australian sandalwood trade. The Australian Government continues to establish guidelines with source countries[37] to ensure businesses apply due diligence in relation to timber importations through compliance assessments.

Australia is currently an exporter of hazardous waste, in particular e-waste. Illegal domestic dumping of e-waste is an ongoing problem. The extent of organised crime involvement in this market is unknown, but there have been reported incidents of organised crime involvement in illegal dumping of hazardous building materials and other waste.

The global trade in illicit ozone-depleting substances (ODS) has been reduced by the successful *Montreal Protocol on Substances that Deplete the Ozone Layer*. Internationally, the illegal trade in hydrochlorofluorocarbons continues to develop. It is unclear if a market in ODS exists in Australia.

Environmental crime is a diverse and expanding crime market that is both profitable and transnational in nature. The impacts of environmental crime can be long-lasting, and in some instances irreversible.

## INTELLECTUAL PROPERTY CRIME

Intellectual property (IP) crime including piracy, counterfeiting and theft of IP continues to be a significant issue within Australia and overseas. Data published in 2016 by the Organisation for Economic Co-operation and Development (OECD) and the European Union's Intellectual Property Office estimated the global value of counterfeit goods in 2013 to be US$461 billion, with China listed as the top producer of counterfeit goods. In October 2016, counterfeit skincare goods to the value of A$150,000 marked with the 'Australian Made' logo were intercepted by the DIBP on a shipment from China.

Instances of cyber-enabled IP crime continue to be detected. For example, in the 10-month period to March 2016, online brand protection and domain name management specialists NetNames removed 2,163,694 counterfeit Billabong Group brand items from online channels.

### CASE STUDY: DIRECT IMPACT OF IP THEFT ON AN AUSTRALIAN BUSINESS

Adelaide-based communications, metal-detection and mining technology firm Codan was subjected to IP theft after Chinese hackers stole designs for metal detection units in 2012. The impact of this breach led to the company's net profit falling from A$45 million in the 2012–13 financial year to A$9.2 million in the 2013–14 financial year.

37 Australia had country-specific guidelines with Canada, Finland, Indonesia, Italy, Malaysia, New Zealand, Solomon Islands, and Papua New Guinea as of March 2016.

# CRIMES AGAINST THE PERSON

## THEME SUMMARY

Crimes against the person include the sexual exploitation of children, human trafficking and slavery. Measuring the extent and financial cost of such crimes is difficult, and this is compounded by under-reporting. In 2013–14, the then Australian Crime Commission conservatively estimated the cost at A$89 million. However, this figure does not factor in the social, health and welfare costs for victims and their families, and represents a partial estimate at best. Severe and long-term psychological, physical and behavioural harms have been reported in victims. Investigations are often made more complex by offences occurring in multiple jurisdictions, domestically and overseas.

The online sexual exploitation of children is a global crime market that is evolving rapidly alongside technological advances. Sophisticated criminal groups and individual offenders increasingly exploit anonymous networks and encryption tools to engage in child sex offences. Offenders are often early adopters of new technologies, and the uptake of mobile and data technology by younger people enables unprecedented online access to children.

Human trafficking and slavery is a global concern, and the mass movement of refugees and migrants in the last two years has escalated the threat. While under-reporting is endemic within this crime type, increased outreach and awareness programs funded by the Australian Government have likely contributed to a growth in referrals to law enforcement for these offences.

## SEXUAL EXPLOITATION OF CHILDREN

The number of reports to Australian law enforcement relating to child sexual exploitation (CSE) and the availability of child exploitation material (CEM) has increased. These crimes are enabled by technological advancements in mobile phones that provide increased numbers of platforms to access CEM, by an overall increased availability of online CEM, and by greater access to encryption and anonymity tools to disguise online activities. The uptake of social media platforms and online game forums, combined with a growth in access to broadband internet and mobile phones, provides unprecedented access to children online. Australia's Office of the Children's eSafety Commissioner reportedly conducted 7,400 investigations into online child sexual abuse content in 2016, with the vast majority of content displaying images of children of primary school age or younger. The rapid evolution of social media and gaming platforms poses challenges in monitoring online safety of children.

The infiltration of legitimate websites by offenders for child grooming, for child sex extortion ('sextortion') and for the dissemination of CEM is an increasing trend. Child sextortion—where children are deceived or coerced into providing sexually comprising imagery, and then extorted to provide more explicit images or money—is likely under-reported due to the victim's fear and shame. Sextortion may also be related to grooming children for the purposes of committing a contact offence.

## CASE STUDY: OFFENDER ARRESTED FOR CEM AND CSE OFFENCES

A South Australian child protection officer was convicted and sentenced to 35 years imprisonment in August 2015 for sexually abusing seven children in his care. The children were predominantly aged between 18 months and three years. The offender was also identified as the head administrator of a sophisticated global CEM network with approximately 1,000 members.

Child exploitation investigations frequently traverse physical borders. Australian offenders are commonly involved as online members, customers, administrators and/or organisers of online global networks featuring CEM. Collaboration between Europol and the AFP using victim identification techniques recently led to the arrest of an Australian man, who had abused two young relatives and his twin baby girls, who were born through surrogacy arrangements. The man subsequently pleaded guilty to 38 charges, including trafficking children, incest, and producing, accessing or transmitting child abuse material and was sentenced to 22 years in prison.

Online CEM is frequently exchanged through peer-to-peer networks. Forums and networks on the darknet that facilitate CEM exchange are growing in number as users become more technologically proficient. Membership to CEM sites can reportedly require regular production and uploading of new CEM, effectively increasing the volume of material available. Methodologies to evade and hinder law enforcement attention are shared by offenders within these forums. Tools such as internet protocol anonymisation, device and communication encryption, cloud storage, and wiping software are often employed by offenders to avoid detection. The involvement of the darknet in the production and distribution of CEM will continue to grow. Disruption of the top-tier members of online CEM sites actively involved in the production, supply and distribution of new CEM on the darknet is an ongoing focus for law enforcement.

Live online streaming of child sexual abuse to paying customers through video-sharing platforms is an emerging issue that is targeting regions with widespread poverty, limited child protection measures and increased access to the internet. The South-East Asia region is known to be targeted by travelling Australian child sex offenders. Offending can comprise either short-stay opportunistic events or long-term embedded offending, and/or online child exploitation. AFP notifications to foreign jurisdictions of pending travel by known Australian child sex offenders[38] aim to reduce offending. Border restrictions for registered child sex offenders, such as passport cancellations and international denial of entry, could potentially lead to an increase in live online streaming of abuse. The sexual exploitation of children will continue to be an issue, and the online environment continues to present challenges in detection as technological advancements in anonymisation and encryption tools are increasingly utilised by offenders.

38 Recorded in the Australian National Child Sex Offender System.

# HUMAN TRAFFICKING AND SLAVERY

Human trafficking and slavery offences include the movement of persons, either domestically or internationally, for the purposes of exploitation and the subjection of persons to exploitative practices including servitude, forced labour and forced marriage.

Human trafficking differs from people smuggling, where people are moved across borders in an organised but irregular manner using a fee-for-service arrangement that does not involve ongoing exploitation.

On an international scale, the exploitation of vulnerable people by human traffickers has significantly escalated in the last two years, due to the mass movement of refugees and migrants as part of the global refugee crisis. When compared to global trends, incidents of human trafficking and slavery in Australia remain uncommon. This is likely explained by a range of factors including strong migration controls, workforce regulations, law enforcement and compliance programs as well as Australia's geographical isolation. Australian Government initiatives including the *National Action Plan to Combat Human Trafficking and Slavery 2015–19* have also played a key role.

The extent of human trafficking and slavery is difficult to quantify and is likely to be under-reported. Successful prosecutions are limited, due both to the complexity of such investigations and the reluctance of victims to speak out. Victims of sexual exploitation have historically dominated referrals for investigation in Australia. Referrals of forced marriage and labour exploitation in the construction, hospitality and domestic service industries have increased and now outnumber referrals relating to sexual exploitation. The AFP received 169 human trafficking referrals in 2015–16, 130 of which related to forms of exploitation outside of the sex industry.

The increase in the number of referrals to the AFP for human trafficking and slavery offences may be, in part, a result of recent legislative amendments. In February 2013, the Australian Parliament passed the *Crimes Legislation Amendment (Slavery, Slavery-like Conditions and People Trafficking) Act 2013*, which made forced marriage a crime punishable by a jail sentence of four to seven years. Since this legislation was passed, the number of referrals to the AFP for investigations into forced marriage and to the Australian Government's Support for Trafficked People Program has risen. Legislative changes introduced in 2015 have further increased the penalties for forced marriage. Additional funding to non-government organisations to administer outreach and awareness-raising programs has also likely contributed to a greater number of referrals. Within the context of forced marriage, Australia's human trafficking profile may change to both a destination and source country. In those few instances identified by the Australian Government where young girls from Australia are taken overseas to marry, the primary offenders are often family members.

Small opportunistic crime groups are more likely to be involved in human trafficking and slavery offences in Australia than large organised crime groups, and typically use overseas family and business contacts to recruit and facilitate the movement of people. Victims often share similar cultural, language, employment and socio-economic backgrounds with offenders.

The visa framework for human trafficking and slavery victims was amended in 2015. The reforms included changes to visa titles to minimise stigmatisation of victims and increase their access to government support and benefits.

While human trafficking and exploitation of vulnerable people in Australia is uncommon, the impact on the individual is significant. The Australian Government remains committed to preventing human trafficking and slavery through the detection and prosecution of offenders, and to providing support for trafficked people.

© Commonwealth of Australia 2017